BUNDESREPUBLIK DEUTSCHLAND

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen:	102 26 744.8
Anmeldetag:	14. Juni 2002
Anmelder/Inhaber:	T-Mobile Deutschland GmbH, Bonn/DE
Bezeichnung:	Content- und Security Proxy in einem Mobilkommunikationssystem
IPC:	H 04 Q 7/20

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 17. Juli 2003
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Ebert

14.06.2002

T-Mobile Deutschland GmbH

Content- und Security Proxy in einem Mobilkommunikationssystem

Die Erfindung betrifft ein Verfahren und eine Einrichtung zur Bereitstellung von Sicherheitsfunktionen bei der Übertragung von Daten von und zu einem Teilnehmerendgerät eines Mobilkommunikationsnetzes.

Aktuelle und neue Datendienste bieten den Teilnehmern von Mobilkommunikationsnetzen einen direkten Zugang zum Internet und anderen öffentlichen Datennetzwerken. Dadurch ist das für den mobilen Einsatz verwendete Mobiltelefon und mit diesem betriebene Zusatzgeräte, wie z.B. ein Notebook oder Personal Digital Assistent, ähnlich wie auch bei einem festnetzbasierten Internetzugang, den verschiedensten Angriffen Dritter ausgeliefert.

Die Aufgabe der Erfindung ist es, ein Verfahren und eine Einrichtung zur Bereitstellung von Sicherheitsfunktionen bei der Übertragung von Daten von und zu einem Teilnehmerendgerät eines Mobilkommunikationsnetzes anzugeben, um das Teilnehmerendgerät und angeschlossene oder mit diesem kombinierte Geräte wirkungsvoll zu schützen.

Diese Aufgabe wird durch die Merkmale der unabhängigen Patentansprüche gelöst.

Der Kern der Erfindung liegt darin, in einem Mobilfunknetz individuell pro Mobilfunkanschluss und Teilnehmer einen personalisierbaren Sicherheitsdienst anzubieten.

Der Teilnehmer kann seine Sicherheitseinstellungen interaktiv und dynamisch anpassen

Vom Netzwerkbetreiber können eine Reihe von sinnvollen Standard-Einstellungen für die Filterfunktionen, z.B. Virenschutz, Schutz vor Werbe-Mails, etc., vorgegeben sein.

Die Schutzfunktion wird dabei von einer netzwerkspezifischen Einrichtung in Form einer Sicherheits- und Filtereinrichtung angeboten. Die generelle Schutzfunktion lässt sich darüber hinaus mit einer Speicherfunktion koppeln, d.h. der Datenverkehr Teile davon werden temporär in der Einrichtung gespeichert und können vom Teilnehmer abgerufen werden. Somit kann die Sicherheits- und Filtereinrichtung zusätzlich die Funktion eines sogenannten Proxy übernehmen. 'Proxy' bedeutet soviel wie 'Stellvertreterdienst'. Proxies nehmen Anforderungen von einem Client, z.B. einem Endgerät, entgegen und geben sie, gegebenenfalls modifiziert, an das ursprüngliche Ziel, z.B. einen Internetanbieter, weiter. Proxies können die durchgeschleusten Daten lokal ablegen und beim nächsten Zugriff direkt liefern.
Damit wird gleichzeitig eine Performance-Steigerung erreicht da bestimmte Inhalte gepuffert werden können.

Erfindungsgemäß können vom beschriebenen System folgende Schutzfunktionen angeboten werden:

Eine Filterung des Datenverkehrs auf IP/TCP Basis in Form einer sogenannten Firewall Funktion. Ferner das Filtern / Abwehren von Datenpaketen bestimmten Ursprungs (IP Adresse) bzw. Datenpaketen von und zu bestimmten Diensten (TCP-Ports).

Eine Analyse des Dateninhalts auf bösartige oder sicherheitskritische Inhalte. Der gesamte Inhalt einer Datenverbindung wird analysiert und nach bestimmten Mustern

untersucht. Signaturen von Viren etc. werden aufgespürt und unschädlich gemacht, bevor sie das Endgerät des Teilnehmers erreichen.

Eine Analyse des Dateninhalts auf unerwünschte Inhalte, z.B. in Form von Spam, Werbung oder anstößigen Inhalten. Hierzu wird der gesamte Inhalt der Verbindung analysiert und vom Teilnehmer angegebener unerwünschter Inhalt wird ausgefiltert, z.B. zum Schutz von Kindern und Jugendlichen.

Der Netzwerkbetreiber selbst kann die Mechanismen des Systems nutzen, um für bestimmte Teilnehmer gezielt bestimmten Datenverkehr auszuschalten, z.B. kostenpflichtige Dienste, wenn Teilnehmer den Dienst nicht subskribiert hat.

Die Filterfunktion für den Dateninhalt kann sinnvoll und technisch mit den selben Mechanismen zusätzlich mit folgenden Funktionen angereichert werden.

Z.B. ist relativ einfach eine Limitierung des Datentransfervolumens realisierbar. Hierzu wird der gesamte Verkehr, unter Umständen getrennt nach kommendem und gehendem Verkehr, aufsummiert und weiterer Verkehr bei Überschreiten eines vom Benutzer oder Betreiber vorgegebenen Limits unterbunden.

Zusätzlich kann mit einer Komponente zur Berechnung der Entgelte die Budget-Einhaltung überprüft werden. Die Teilnehmer bzw. der Betreiber kann eine bestimmte Obergrenze für die Kommunikationskosten vorgeben. Bei Überschreitung des festgelegten Budgets wird der Teilnehmer benachrichtigt und der Datenverkehr unterbunden. Damit ist eine effektive Kostenkontrolle und Kostentransparenz möglich.

Weitere Funktionen können sinnvoll in das System integriert werden:

Treten bestimmte Ereignisse ein, d.h. werden Angriffe erkannt, Spam-Mails gefiltert oder ähnliche Ereignisse vom System erkannt, erfolgt die Benachrichtigung des

Teilnehmers oder Netzbetreibers um eine transparente Kontrolle der ausgefilterten Daten zu ermöglichen.

Der Teilnehmer kann weiterhin administrieren, ob sein gesamter Verkehr über das System geleitet wird oder nur selektiv, d.h. zu bestimmten Zeiten, nach entsprechenden Vorfällen oder bei Missbrauchsverdacht.

Gemäß einer Weiterbildung der Erfindung kann eine verteilte Realisierung der Filterfunktionen vorgesehen sein, d.h. die Sicherheits- und Filtereinrichtung ist nicht zentral in einem Netzknoten des Mobilkommunikationssystems vorgesehen, sondern verteilt oder individuell in mehreren Netzknoten. Damit wird die Last für den einzelnen Knoten verringert.

Dies Einrichtung des Systems kann

(a) entweder räumlich oder netzwerktechnisch bedingt sein, d.h. Verteilung auf mehrere Netze oder Netzknoten, oder

(b) funktional bedingt sein, z.B. spezielle Filterkomponenten für bestimmte Dateninhalte, z.B. Email-Filter, Virenfilter, etc., oder

(c) architektonisch oder softwaretechnisch bedingt sein, aufgrund z.B. einer Verwendung spezieller Hardware und Systemsoftware für bestimmte Funktonen.

Die Administration dieser zusätzlichen Funktionen kann jeweils zentral von einem bestimmten Knoten aus erfolgen.

Ein Ausführungsbeispiel der Erfindung wird nachfolgend anhand einer Zeichnungsfigur beschrieben.

Figur 1 zeigt schematisch die technische Ausgestaltung des Systems.

Das System ist Teil eines Mobilkommunikationsnetzes 10, welches einer Vielzahl von Teilnehmerendgeräten 13 die Kommunikation mit anderen öffentlichen Netzen, z.B. dem Internet 11, erlaubt.
Ferner können an das Mobilfunkendgerät 13 angeschlossene, kombinierte Geräte 14, wie z.B. PC, PDA, Smartphone, etc. vorgesehen sein, die eine komfortable mobile Internetnutzung ermöglichen.

Innerhalb des Mobilkommunikationsnetzes 10, vorzugsweise innerhalb eines entsprechenden Netzknotens, wie z.B. einer Vermittlungsstelle MSC, ist die erfindungsgemäße Sicherheits- und Filtereinrichtung 1 angeordnet, die erfindungsgemäß aus folgenden funktionalen Teilen bestehen kann.

Die generelle Filterkomponente 2:
Diese Komponente hat eine vom Teilnehmer / Netzbetreiber definierbare variable Filterfunktion und untersucht in Echtzeit den zwischen dem Endgerät 13 des Teilnehmers und dem Internet 11 ausgetauschten Datenstrom 12. Der Teilnehmerverkehr 12 in beide Richtungen geht über diesen Filter 2 und wird dort analysiert.

Die Authentikationskomponente 3:
Zur Benutzung der Sicherheits- und Filtereinrichtung 1 muss sich der Teilnehmer gegenüber dem System authentisieren. Damit wird sichergestellt, dass kein unautorisierter Zugriff auf z.B. die persönlichen Einstellungen des Teilnehmers erfolgen. Die Authentikation kann im einfachsten Fall über die Rufnummer MSISDN des Teilnehmers erfolgen. Sicherer und besser geschützt wird der Teilnehmer mit einer zusätzlichen PIN oder einem Passwort.
Gegebenenfalls kann ein kryptographisches Authentikationsverfahren benutzt werden, z.B. Zertifikate des Teilnehmers.

Die Administrationskomponente 4:

Diese Komponente bildet die Schnittstelle zwischen dem System und dem Teilnehmer. Hier kann der Teilnehmer seine persönlichen Einstellungen administrieren. Dies kann direkt über das Mobilfunksystem, das Internet oder festnetzbasierte Kunden-Schnittstellen des Netzbetreibers erfolgen.

Die Datenbasis 5:
Die Datenbasis 5 beschreibt, welche Daten durch die Filterkomponente 2 auszufiltern oder zu bearbeiten sind. Diese Datenbasis 5 kann vorteilhaft in vier Datenbanken aufgeteilt werden. Die erste Datenbank 6 enthält die individuellen Filter und Einstellungen pro Teilnehmer. Die zweite Datenbank 7 enthält die Filter und Einstellungen pro Mobiltelefon-Typ.
Die dritte Datenbank 8 enthält die netzbetreiberspezifischen Einstellungen und Filter, und die vierte Datenbank 9 enthält die allgemeinen Einstellungen und Filter.

Patentansprüche

1. Verfahren zur Bereitstellung von Sicherheitsfunktionen bei der Übertragung von Daten von und zu einem Teilnehmerendgerät eines Mobilkommunikationsnetzes, **dadurch gekennzeichnet,**
dass in einer Einrichtung (1) eines Netzwerkknoten des Mobilkommunikationsnetzes (10) eine Echtzeit-Analyse des Datenstroms (12) von und zu dem Teilnehmerendgerät (13) durchgeführt wird, wobei Daten mit zuvor vom Teilnehmer oder einem Netzbetreiber / Provider definierten Inhalten erkannt und weiterverarbeitet werden.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass der Datenverkehr von und zu definierten Absendern und Empfängern erkannt und weiterverarbeitet werden.

3. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die erkannten Daten selektiert und/oder isoliert und/oder gelöscht und/oder dem Teilnehmer oder Netzbetreiber / Provider separat zur weiteren Verarbeitung zu Verfügung gestellt werden.

4. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass eine Filterung insbesondere des IP/TCP basierten Datenverkehrs durchgeführt wird.

5. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass das anfallende Datentransfervolumen auf ein vom Teilnehmer oder dem Netzbetreiber festgesetztes Maß limitiert wird.

6. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die anfallenden Datenübertragungskosten auf ein vom Teilnehmer oder dem Netzbetreiber festgesetztes Maß limitiert wird.

7. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass der Teilnehmer, Netzbetreiber oder Provider bei Erkennung von bestimmten Dateninhalten und/oder Absendern benachrichtigt wird.

8. Einrichtung zur Bereitstellung von Sicherheitsfunktionen bei der Übertragung von Daten von und zu einem Teilnehmerendgerät eines Mobilkommunikationsnetzes, umfassend eine Sicherheits- und Filtereinrichtung (1) mit folgenden Komponenten:
eine Filterkomponente (2) zur Echtzeit-Analyse des Datenstroms von und zu dem Teilnehmerendgerät;
einer Authentikationskomponente (3) zur Authentisierung des Teilnehmers gegenüber der Sicherheits- und Filtereinrichtung;
einer Administrationskomponente (4) als Schnittstelle zum Teilnehmer;
eine Datenbasis (5) zur Speicherung von teilnehmer- und netzbetreiberspezifischen Daten sowie von Sicherheits- und Filterfunktionen.

9. Einrichtung nach Anspruch 9, dadurch gekennzeichnet, dass die Sicherheits- und Filterkomponente (2) in einem oder mehreren Netzknoten des Mobilkommunikationsnetzes (10) eingerichtet ist.

10. Einrichtung nach Anspruch 9 oder 10, dadurch gekennzeichnet, dass für bestimmte Dateninhalte spezielle Filterkomponenten eingerichtet sind.

Zusammenfassung

Die Erfindung betrifft ein Verfahren und eine Einrichtung zur Bereitstellung von Sicherheitsfunktionen bei der Übertragung von Daten von und zu einem Teilnehmerendgerät eines Mobilkommunikationsnetzes. In einer Einrichtung eines Netzwerkknoten des Mobilkommunikationsnetzes wird eine Echtzeit-Analyse des Datenstroms von und zu dem Teilnehmerendgerät durchgeführt, wobei Daten mit zuvor vom Teilnehmer oder einem Netzbetreiber / Provider definierten Inhalten erkannt und weiterverarbeitet werden.
Dadurch wird das Endgerät und daran angeschlossene Geräte des Teilnehmers bestmöglich gegen Angriffe von außen geschützt.

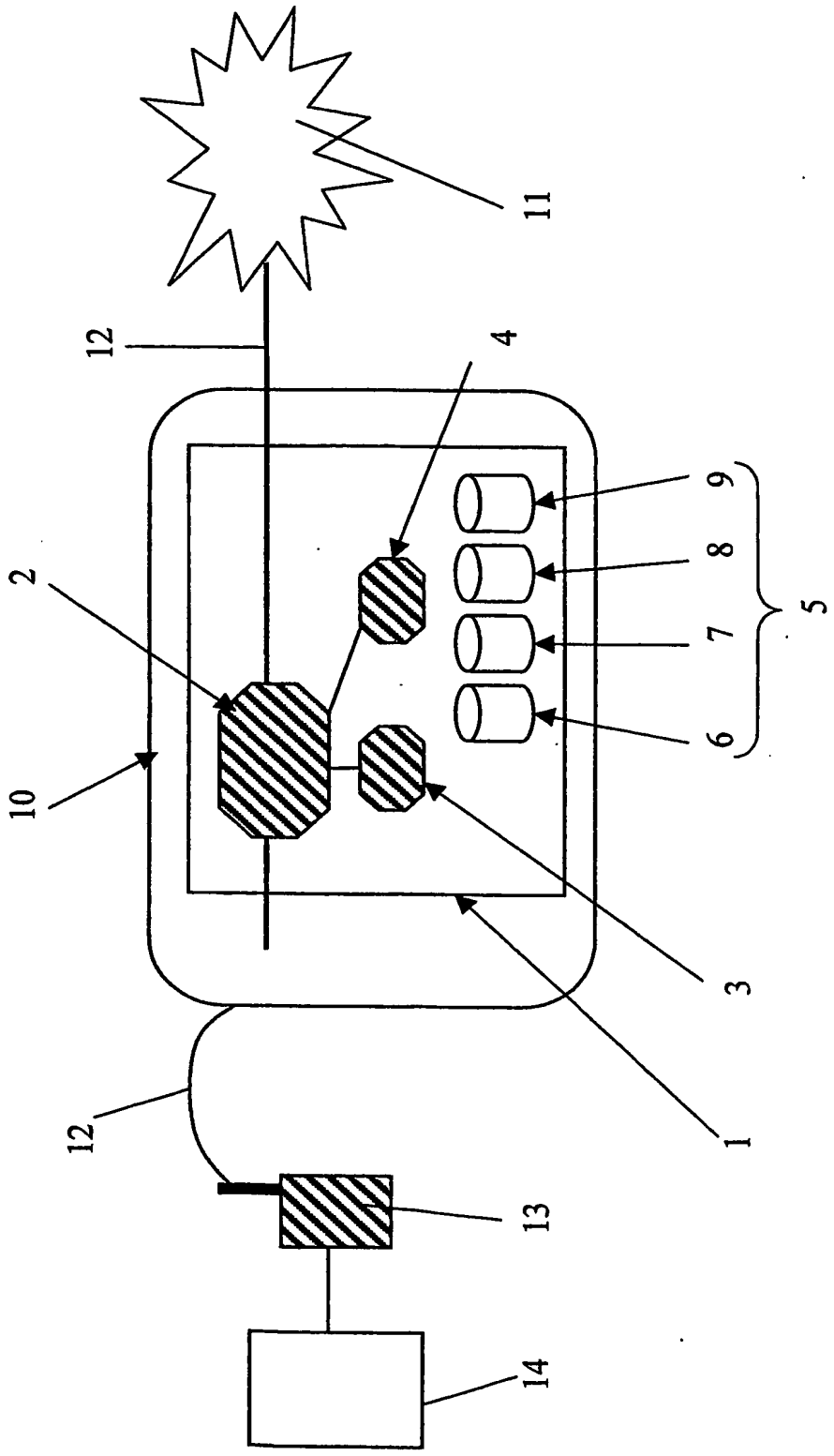

Fig. 1